HEWLETT-PACKARD COMPANY
Legal Department, 20BN
P.O. Box 10301
Palo Alto, California 94303-0890

PATENT APPLICATION

ATTORNEY DOCKET NO. 10980822-1

IN THE U.S. PATENT AND TRADEMARK OFFICE
Patent Application Transmittal Letter

05/15/98

ASSISTANT COMMISSIONER FOR PATENTS
Washington, D.C. 20231

Sir:

Transmitted herewith for filing under 37 CFR 1.53(b) is a(n): (X) Utility   ( ) Design

(X) original patent application,

( ) continuation-in-part application

INVENTOR(S): **Teddy C. Johnson**

TITLE: **High-Performance Server Data Delivery System and Method**

Enclosed are:

(**X**) The Declaration and Power of Attorney.   (**X**) signed   ( ) unsigned or partially signed

(**X**) _____ sheets of drawings (one set)

( ) Information Disclosure Statement and Form PTO-1449   ( ) Associate Power of Attorney

( ) Priority document(s) ( ) (Other) _____   (fee $_____)

CLAIMS AS FILED BY OTHER THAN A SMALL ENTITY						
(1) FOR	(2) NUMBER FILED		(3) NUMBER EXTRA	(4) RATE	(5) TOTALS	
TOTAL CLAIMS	11 —	20	0	X $ 22	$	0
INDEPENDENT CLAIMS	3 —	3	0	X $ 82	$	0
ANY MULTIPLE DEPENDENT CLAIMS	0			$ 270	$	0
BASIC FEE: Design ($330.00); Utility ($790.00)					$	790
TOTAL FILING FEE					$	790
OTHER FEES					$	0
TOTAL CHARGES TO DEPOSIT ACCOUNT					$	790

Charge $_____790_____ to Deposit Account 08-2025. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16, 1.17,1.19, 1.20 and 1.21. A duplicate copy of this sheet is enclosed.

"Express Mail" label no. EE324737955US

Date of Deposit 6/5/98

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to: Assistant Commissioner for Patents, Washington, D.C. 2023

By _____

Typed Name: **Dianna Baker**

Respectfully submitted,

Teddy C. Johnson

By _____

Jeffrey D. Wheeler

Attorney/Agent for Applicant(s)
Reg. No.   **39,066**

Date: **6/5/98**

Telephone No.: **408-553-3040**

HIGH PERFORMANCE SERVER DATA
DELIVERY SYSTEM AND METHOD

FIELD OF INVENTION

This invention relates to a secure, high-throughput,
scalable apparatus and method of downloading software
products and other data to authorized customers over the
internet.

BACKGROUND OF THE INVENTION

Presently software is sold and shipped via electronic
and optical storage mediums such as floppy disks and compact
disks. Such methods require physical duplication and
shipment of new products to customers. This adds
considerable expense, particularly when data products change
or are updated periodically. In order to have current
information, a user might need to frequently receive new
software revisions.

Accordingly, the internet is fast becoming a preferred
medium for information transfer, and new types of low cost
equipment are continually being developed to connect users to
the ever-growing number of websites. Access to a particular
website is managed by a host server or router. External
parties, or customers, typically contact the site via use of
an internet browser to access a known URL (uniform resource
locator). The website might be constructed so as to provide

1

downloading access to programs or data, either on or through that host server, to customers contacting that site.

Prior configurations or solutions for downloading software from a website include possible drawbacks which affect the speed and security of the transfer. Security measures include firewalls which are hardware and/or software barriers which prevent access to certain isolated machines or programs within a network or system. Prior downloading configurations typically use one machine (or server), which is accessible externally to the firewall, which includes a web server, an ftp (file transport protocol) server, a database containing customer account information, a secured data repository, and customer download areas. Prior configurations have typically chosen to download or deliver software from the same machine which is hosting the web server. Software can take a considerable time to prepare, or stage, for secure download to a customer, as the software is often physically copied from a secure area, on one side of a firewall, into a new area which is accessible by an external customer. The speed of such transfers is also affected by the requirement that the host server is often required to process too many tasks at the same time. Yet another time-consuming step might involve the requirement that customers be pre-configured on a certain database (external to the firewall) in order to access particular information.

2

In particular, a customer might typically use a web browser to access a well known URL, and then perform an authentication process using a username/password pair. The web browser might then backend script the information by

5   invoking a cgi-bin (common gateway interface -- binary) in order to check a customer account database to verify that the customer should be allowed access. The customer might then request a software download. The web server cgi-bin further checks the customer account in order to verify that the user

10   is entitled to the particular requested software. Upon passing a validation check, the requested software is then copied from a secured file repository to a secured ftp account for this customer (e.g. secured via a Unix change root, or chroot, command). The web server then delivers an

15   HTML (hypertext markup language) page to the customer's browser. When the user activates the ftp://URL on that page, the web browser communicates with the ftp server on that host, and the software download commences.

A primary drawback to this approach is that it severely

20   slows down the web server performance, which typically displeases customers. Software files are generally very large (e.g. 10 to 100 Megabytes per download). During a software download, the web server's CPU cycles and network bandwidth must be shared with the ftp server. The ftp server

25   uses considerable resources, as it must read the file from a

disk storage area, and then send it out through a connection
medium, for instance a LAN (local area network) card, to the
client web browser.

Web server performance is further degraded because the

5 standard method for making sure the customer only receives
certain software (to which they are entitled) is generally
very expensive to implement. One standard method is to
create a custom change root ftp directory for the customer,
and then to copy the software from a secure repository into

10 that account. Under the preferred UNIX operating system, a
chroot (change root) command achieves this objective.
Methods involving symbolic links cannot be used, because
symbolic links do not work in conjunction with a chroot
command. The copying operation is extremely resource

15 intensive, and gets more expensive in direct proportion to
the size of the requested software object or file.

Another drawback of the prior solutions is that
customers must be pre-configured into an external account
database. The presents a synchronization problem in that the

20 external database must contain customer information before
the customer will be allowed access. The database also needs
to be regularly updated to ensure that it contains the
correct status of the customer account.

Hence, what is needed in the field is a solution for

25 providing fast software delivery without impacting web server

performance. This solution should also incorporate secure communications between host machines, fast file staging for software downloads, an dynamic user authentication through a firewall.

5

SUMMARY OF THE INVENTION

The invention described herein provides a secure, high-throughput, scalable system and method of downloading software products and other data to authorized customers over the internet. The system uses separate machines for web server operations and ftp server operations in order to speed up performance. A secure mechanism for communicating between the two machines is used in order to properly stage the software for download. The secure mechanism utilizes a pair of client/server programs which use TCP (transmission control protocol), DES (data encryption standard), a filter to render the cypher string safe, and a secure method of passing DES keys.

A fast file staging mechanism is used to which enables software to be staged very quickly (e.g. less than one second), regardless of the size of the software object. Rather than physically copying software from a storage area to a staging area, a hard link is created between the customer's ftp account and the secure repository.

25

The present invention also eliminates the need for an external customer account database via use of the secure commlink in conjunction with the tobj (tagged object) protocol. Tobj is a Hewlett-Packard SGML (standard Graphics Markup Language) style of data encapsulation protocol which implemented on top of standard protocols and which sends transactions across a specified range of ports. A master database of customer access information is maintained inside the firewall, with data crossing the firewall in a secure fashion.

Other advantages of this invention will become apparent from the following description taken in conjunction with the accompanying drawings which set forth, by way of illustration and example, certain embodiments of this invention. The drawings constitute a part of this specification and include exemplary embodiments, objects and features of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a prior art server configuration with the host machine running multiple processes external to a firewall.

Figure 2 shows a server configuration of the present invention which separates processes onto multiple machines having a secure communication link (commlink) between them,

6

uses fast file staging, and provides dynamic ftp
authentication with a firewall protected customer database.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention provides a fast and secure method
and system for downloading software, or other data, from a
server configuration. The configuration separates processing
tasks between machines to improve efficiency, yet maintains
system control via a secure commlink between machines. File
staging is provided via direct customer hard links to data
storage areas and customer access is dynamically
authenticated from a secure database.

Figure 1 shows a prior art configuration 10 which
implements multiple processing tasks on one host machine 12.
Such tasks might include, for instance, web server processes
and ftp server processes. Also shown is a storeroom disk
storage area 14 and a customer account disk storage area 16.
When a customer desires a software download, the host machine
12 is contacted through connection 19 by the customer's web
browser 18, via modem and the like, using hypertext transfer
protocols (http). If a software download is desired by the
customer, then the host machine authenticates a customer
account through a customer database. The host machine then
allocates space in the customer storage area 16 and requests
copying of the desired software from the storeroom 14 to the

relevant customer account area 16. When the copying
operation is completed, the ftp server contained on the host
machine 12 provides file transfer to the customer's web
browser 18 via file transfer protocols (ftp).

5   This configuration results in a significant number of
tasks being performed by one host machine 12, and over one
customer/host connection 19. As a result, all of the host
machine processes will be slowed down. Slower web processes
result in customer access lags. Slower ftp processes result

10   in longer file transfers. Limited bandwidth on the
connection 19 results in bottle-necking of data being
transferred to the customer web browser 18. Additionally,
the server configuration 10 is located entirely outside of a
protective firewall 20.

15   Figure 2 shows a server configuration 30 of the present
invention. A host machine 32 is used to handle web server
processes. A separate host machine 34 is used to handle ftp
server processes. A customer web browser 44 communicates via
a communication link 46 (e.g modem or the like) with the web

20   server 32 using http protocol (e.g. via an example URL
http://destination). The customer web browser 44 also
communicates with the ftp server 34 via a communication link
48 using ftp protocol (e.g. URL ftp://destination).

As separate machines 32, 34 are used for the two

25   processes, a link 36 is needed for communicating between the

two machines. Such a link includes, for instance, a LAN (local area network) connection. Data communicated over the LAN is done is a secure manner. The preferred embodiment uses a custom secure TCP protocol, henceforth referred to as the Fulfillment Server Protocol (FFS). This protocol is similar to the Network Virtual Terminal (NVT) protocol (i.e. RFC764, Telnet), in that it specifies a protocol for the exchange of arbitrary sized packets of ascii data, delimited by CR NL (carriage return, newline) boundary markers. However, the FFS Protocol enhances the generic NVT protocol by using DES encryption, applying a filter to render the cipher string 7-bit safe, and using a unique technique for securing passing the associated DES keys, wherein DES uses a known set of keys for encryption and decryption of data streams. The connection 36 between the two machines is therefore referred to as an FFS communications link (commlink) for discussion purposes.

Since the LAN connection between the two machines is potentially subject to filtering by an intruder, it becomes necessary to securely pass the recipient the key to decode the data stream (and to encode the reply). Before the web server and ftp server are first brought on line, the Daemon software is installed on them (daemons are processes that run in the background of a computer). The Daemon software implements the FFS commlink software which has compiled into

9

it a finite set of N DES keys (e.g. a "bag" of keys) 38 which are retrievable by index number.

When one side of the FFS commlink receives an incoming FFS protocol packet, it selects one of the keys out if its bag of N keys 38 to decrypt the packet. The actual key itself is never sent across the LAN connection 36. Instead, it is assumed that the key will be contained within the bag of keys. The method used to select the proper key involves the following steps:

(1) Find the ephemeral port number, P, used for the connection. This port number varies, in a pseudorandom manner, per the implementation of the TCP specification.

(2) Compute the value I, where I = P modulo N.

(3) Use I as the index into the bag of keys, and use the DES key residing at index I to decrypt the request stream of data, and to encrypt the reply stream.

Notably, this is not a weakening of the DES key space. Even though there are only N keys (e.g. 128 keys), an intruder listening on the LAN connection 36 has no way of knowing which of the keys (e.g. potentially 2^{56} keys) have been selected as the particular N keys for usage. Therefore an intruder cannot feasibly decode a packet in the FFS commlink, because the intruder has no idea about which DES key to use. Similarly, it is also virtually impossible to insert a fake packet in the FFS commlink stream, as the

intruder does not know which key to use for the encryption.
This is because no access has been provided to the bag of
keys which were compiled into the code running at the two
endpoint machines 32 and 34.

5   Another feature of the present invention enables the
configuration to stage software for downloading relatively
quickly (e.g. less than one second), regardless of the size
of the software object. For instance, copying requires that
the entire file be read from a safe area or storeroom 40, and
10   then written into a customer account area 42. This might
easily take tens of minutes on an unloaded system for a large
file (e.g. 100 megabytes), and such transfer times might
typically approach an hour or more on a busy system.

When an ftp download is staged for a customer, typically
15   a chroot (change root) ftp account is created for that
customer, and then the requested software is copied into that
customer's ftp account. The chroot command limits a user's
access to that particular directory level on the system.
This provides security by preventing the customer from
20   accessing arbitrary locations in the file system. It would
be preferable to simply provide a symbolic link from the
customer's ftp account 42 and the secure repository 40.
However, due to the nature of the way the chroot command
implements security, symbolic links cannot be properly
25   resolved or utilized.

11

A solution exists in the characteristic implementation
of certain file systems, such as HP-UX HFS (Hierarchical File
System) and JFS (Journal File System), and particularly when
implemented on a redundant array of independent disks 50
(raid). Because of the parallel structure of such raid file
systems, and because of underlying features of the HP-UX file
system, it is possible to create a hard link between the
customer's ftp account area 42 and the secured repository
area 40. This operation takes a trivial amount of time
(typically less than one second), regardless of the size of
the target file. Additionally, this technique provides the
same relative degree of security as the conventional method
of physically copying over the entire file. File space is
saved since there is only one copy of the software object on
the secured storage, rather than several duplicate copies
existing in the various customer directories in storage area
42 (e.g. when two different customers request a download of
the same object file).

Firewalls exist as hardware and software security
measures in network configurations in order to prevent access
to certain isolated machines or programs within the network
or system. Prior systems have typically located customer
authentication databases outside of a firewall 52, thus
leaving proprietary customer access information vulnerable to
external theft and attacks. The FFS architecture has

12

eliminated the need for an external customer account database via use of an FFS secure commlink in conjunction with Tobj protocol. This allows data to cross the firewall 52 in a secure fashion from an internal master database 56 which

5   resides on an internal machine or server 58.

Generally a system 30 should be designed with as few paths, or gateways, through the firewall 52 as possible. This protects proprietary information and the like 60 stored on the internal server 58. The present system uses the web

10   server machine 32 as a proxy to communicate with the ftp server machine 34, and through the firewall 52, as necessary, in order to coordinate transfer of data. Additionally, there is no need to continually synchronize the internal database with an external database.

15   The server configuration(s) depicted and described above are not intended to be limited to the specific components or links shown, and such elements are only meant to illustrate the principles of the overall invention. It is to be understood that while certain forms of the invention are

20   illustrated, they are not to be limited to the specific forms or arrangements of parts herein described and shown. It will be apparent to those skilled in the art that various changes may be made without departing from the scope of the invention and the invention is not to be considered limited to what is

25   shown in the drawings and descriptions.

WHAT IS CLAIMED IS:

1.   1.   An apparatus for facilitating the high speed

2. transfer of data to authorized users over the internet, the

3. apparatus comprising:

4.   a plurality of host machines for running a plurality of

5. processes;

6.   at least one secure communication link between the host

7. machines;

8.   a file storage system having a storeroom area and a

9. customer account area with a hard linking capability there

10. between;

11.   a firewall with at least one secured host machine

12. residing on the secured side of the firewall; and

13.   a customer account database located on the secured host

14. machine and accessible by a secured communication link

15. through the firewall.

1.   2.   The apparatus of Claim 1, wherein the at least one

2. secure communication link utilizes a protocol for the

3. exchange of arbitrary sized packets of ascii data, delimited

4. by carriage return and newline boundary markers.

1.   3.   The apparatus of Claim 2, wherein at least one

2. secure communication link enhances the protocol by utilizing

3. DES encryption with N DES keys, and a method for securely

14

4   passing the DES keys comprising the steps of:

5   (i)   finding the port number P used for the connection;

6   (ii) computing a value I = P modulo N; and

7   (iii) using I as the index into the N keys, and using

8   the DES key residing at index I to encrypt and decrypt the

9   data stream.

1   4.   The apparatus of Claim 3, wherein the DES

2   encryption creates a cypher string, and a filter is applied

3   to render the cypher string at least 7-bit safe.

1   5.   The apparatus of Claim 1, wherein the hard linking

2   capability includes a change root command.

1   6.   The apparatus of Claim 1, wherein the secured link

2   through the firewall utilizes tobj protocol.

1   7.   The apparatus of Claim 1, wherein at least one host

2   machine runs a web server process and at least one separate

3   host machine runs an ftp server process, whereby a customer

4   web browser contacts the host machines.

1   8.   A method of facilitating the high speed transfer of

2   data to authorized users over the internet, the method

3   comprising the steps of:

4   (i) running a web server process on at least one host

5   machine;

6   (ii) running an ftp server process on a separate host

7   machine;

8   (iii) establishing a secure communication link between

9   the host machines;

10   (iv) establishing a hard link between storeroom file

11 storage areas and customer account file storage areas; and

12   (v) dynamically allocating customer access information

13 from a secured database.

1   9.   The method of Claim 8, wherein step (iii) uses a

2   protocol for the exchange of arbitrary sized packets of ascii

3   data delimited by carriage return and newline boundary

4   markers, and using DES encryption with N keys, step (iii)

5   including the following steps:

6   (a) finding the port number P used for the

7   connection;

8   (b) computing an index value I, where I = P modulo

9   N; and

10   (c) using the DES key residing at index I to

11 encrypt and decrypt the data stream.

1   10.   The method of Claim 9, wherein the DES encryption
2   creates a cypher string, and filtering is applied to render
3   the cypher string at least 7-bit safe.

1   11.   An apparatus for facilitating the high speed
2   transfer of data to authorized users over the internet, the
3   apparatus comprising:
4   a plurality of host machine means for running a
5   plurality of processes;
6   at least one secure means for communicating between the
7   host machines;
8   a file storage means having a storeroom area and a
9   customer account area with a means for securely hard linking
10   between the areas;
11   a firewall means for providing security between
12   machines, with at least one secured host machine means
13   residing on the secured side of the firewall;
14   a means for databasing customer accounts located on the
15   secured host machine means and accessible by a secured means
16   for communicating through the firewall.

ABSTRACT

A secure, high-throughput, scalable apparatus and method of downloading software products and other data to authorized customers over the internet. A plurality of processes are run on different host machines. The machines communicate with each other via a secured link. This link uses DES encryption and an index to the DES keys, rather than passing the key itself over the link. Once derived, the indexed key is used for encryption and decryption over the communication link. File staging is accomplished by using a hard link between the file storage area and the customer account area. A customer account database is maintained on a secure machine as protected via a firewall. A secured link is also used through the firewall to securely allocate user access to file downloads.
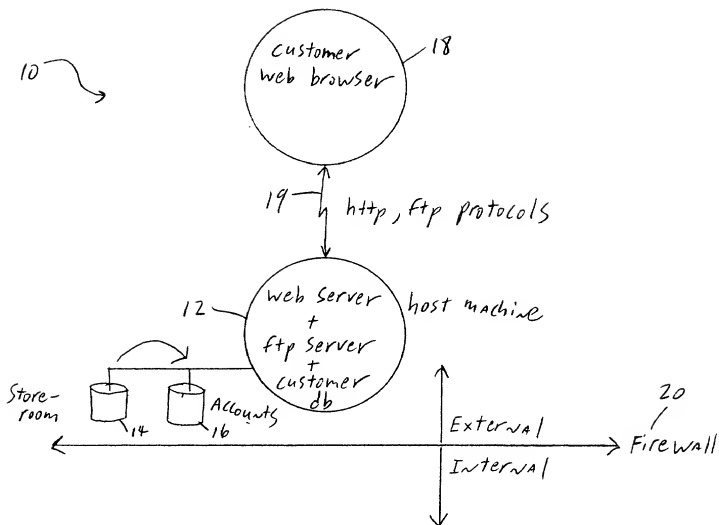
10

customer
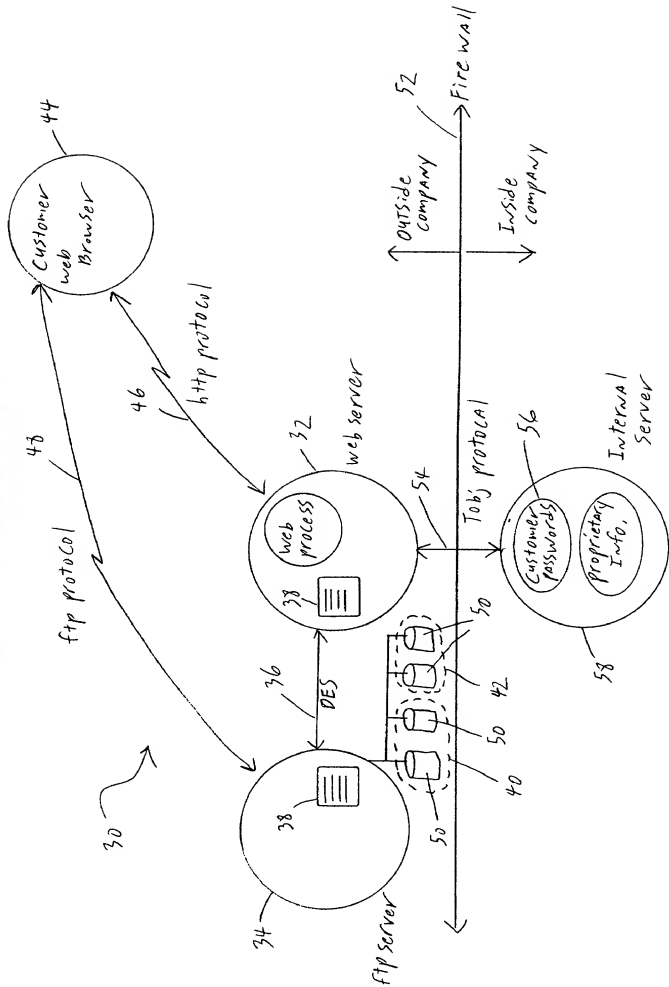web browser   18

19   http, ftp protocols

12   web server
        +
      ftp server   host machine
        +
      customer
         db

Store-
room

Accounts

14   16

External

Internal

20
Firewall

Fig. 1 (prior Art)

Fig. 2

Customer web Browser — 44

ftp protocol — 48

http protocol — 46

web server — 32

web process

DES — 36

ftp server — 34

38

Toby protocol — 54

Outside company

Inside company

Fire wall — 52

Internal Server

Customer Passwords — 56

Proprietary Info.

58

50 42 40 50 50

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION	ATTORNEY DOCKET NO. 10980822-1

As a below named inventor, I hereby declare that:

My residence/post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

High-Performance Server Data Delivery System and Method

the specification of which is attached hereto unless the following box is checked:

( ) was filed on_____as US Application Serial No. or PCT International Application Number _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understood the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56.

Foreign Application(s) and/or Claim of Foreign Priority

I hereby claim foreign priority benefits under Title 35, United States Code Section 119 of any foreign application(s) for patent or inventor(s) certificate listed below and have also identified below any foreign application for patent or inventor(s) certificate having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE FILED	PRIORITY CLAIMED UNDER 35 U.S.C. 119
			YES ____ NO:____
			YES. ____ NO: ____

Provisional Application

I hereby claim the benefit under Title 35, United States Code Section 119(e) of any United States provisional application(s) listed below:

APPLICATION SERIAL NUMBER	FILING DATE

U. S. Priority Claim

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (patented/pending/abandoned)

POWER OF ATTORNEY:

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) listed below to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Jeffrey D. Wheeler	Pamela Lau Kee	John L. Imperato	James C. Pintner
Reg. No. **39,066**	Reg. No. **36,184**	Reg. No. **40,026**	Reg. No. **33,272**

Send Correspondence to:
IP Administration
Legal Department, 20BN
HEWLETT-PACKARD COMPANY
P.O. Box 10301
Palo Alto, California 94303-0890

Direct Telephone Calls To:

Jeffrey D. Wheeler

408-553-3040

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Inventor: **Teddy C. Johnson**   Citizenship: **US**

Residence: **468 Dell Avenue, Mountain View, CA 94043**

Post Office Address: **PO Box 866, Mountainview, CA 94042**

Inventor's Signature   Date **6/5/98**